Assignment 1,2

Types of Cyber Attacks

1. Malware Attack

This is one of the most common types of cyberattacks. “Malware” refers to malicious software viruses including worms, spyware, ransomware, adware, and trojans.

The trojan virus disguises itself as legitimate software. Ransomware blocks access to the network's key components, whereas Spyware is software that steals all your confidential data without your knowledge. Adware is software that displays advertising content such as banners on a user's screen.

Malware breaches a network through a vulnerability. When the user clicks a dangerous link, it downloads an email attachment or when an infected pen drive is used.

2. Phishing Attack

Phishing attacks are one of the most prominent widespread types of cyberattacks. It is a type of social engineering attack wherein an attacker impersonates to be a trusted contact and sends the victim fake mails.

Unaware of this, the victim opens the mail and clicks on the malicious link or opens the mail's attachment. By doing so, attackers gain access to confidential information and account credentials. They can also install malware through a phishing attack.

3. Man-in-the-Middle Attack

A Man-in-the-Middle Attack (MITM) is also known as an eavesdropping attack. In this attack, an attacker comes in between a two-party communication, i.e., the attacker hijacks the session between a client and host. By doing so, hackers steal and manipulate data.

As seen below, the client-server communication has been cut off, and instead, the communication line goes through the hacker.

4. SQL Injection Attack

A Structured Query Language (SQL) injection attack occurs on a database-driven website when the hacker manipulates a standard SQL query. It is carried by injecting a malicious code into a vulnerable website search box, thereby making the server reveal crucial information.

This results in the attacker being able to view, edit, and delete tables in the databases. Attackers can also get administrative rights through this.

5. Denial-of-Service Attack

A Denial-of-Service Attack is a significant threat to companies. Here, attackers target systems, servers, or networks and flood them with traffic to exhaust their resources and bandwidth.

When this happens, catering to the incoming requests becomes overwhelming for the servers, resulting in the website it hosts either shut down or slow down. This leaves the legitimate service requests unattended.

It is also known as a DDoS (Distributed Denial-of-Service) attack when attackers use multiple compromised systems to launch this attack.

6. Watering Hole Attack

The victim here is a particular group of an organization, region, etc. In such an attack, the attacker targets websites which are frequently used by the targeted group. Websites are identified either by closely monitoring the group or by guessing.

After this, the attackers infect these websites with malware, which infects the victims' systems. The malware in such an attack targets the user's personal information. Here, it is also possible for the hacker to take remote access to the infected computer.

7. Whale-phishing Attacks

A whale-phishing attack is so-named because it goes after the “big fish” or whales of an organization, which typically include those in the C-suite or others in charge of the organization. These individuals are likely to possess information that can be valuable to attackers, such as proprietary information about the business or its operations.

If a targeted “whale” downloads ransomware, they are more likely to pay the ransom to prevent news of the successful attack from getting out and damaging their reputation or that of the organization. Whale-phishing attacks can be prevented by taking the same kinds of precautions to avoid phishing attacks, such as carefully examining emails and the attachments and links that come with them, keeping an eye out for suspicious destinations or parameters.

8. Ransomware

With ransomware, the victim’s system is held hostage until they agree to pay a ransom to the attacker. After the payment has been sent, the attacker then provides instructions regarding how the target can regain control of their computer. The name "ransomware” is appropriate because the malware demands a ransom from the victim.

In a ransomware attack, the target downloads ransomware, either from a website or from within an email attachment. The malware is written to exploit vulnerabilities that have not been addressed by either the system's manufacturer or the IT team. The ransomware then encrypts the target's workstation. At times, ransomware can be used to attack multiple parties by denying access to either several computers or a central server essential to business operations.

9. DNS Spoofing

With Domain Name System (DNS) spoofing, a hacker alters DNS records to send traffic to a fake or "spoofed" website. Once on the fraudulent site, the victim may enter sensitive information that can be used or sold by the hacker. The hacker may also construct a poor-quality site with derogatory or inflammatory content to make a competitor company look bad.

In a DNS spoofing attack, the attacker takes advantage of the fact that the user thinks the site they are visiting is legitimate. This gives the attacker the ability to commit crimes in the name of an innocent company, at least from the perspective of the visitor.

To prevent DNS spoofing, make sure your DNS servers are kept up-to-date. Attackers aim to exploit vulnerabilities in DNS servers, and the most recent software versions often contain fixes that close known vulnerabilities.

10. Eavesdropping Attacks

Eavesdropping attacks involve the bad actor intercepting traffic as it is sent through the network. In this way, an attacker can collect usernames, passwords, and other confidential information like credit cards. Eavesdropping can be active or passive.

With active eavesdropping, the hacker inserts a piece of software within the network traffic path to collect information that the hacker analyzes for useful data. Passive eavesdropping attacks are different in that the hacker "listens in," or eavesdrops, on the transmissions, looking for useful data they can steal.

Both active and passive eavesdropping are types of MITM attacks. One of the best ways of preventing them is by encrypting your data, which prevents it from being used by a hacker, regardless of whether they use active or passive eavesdropping.

II.

Monolithic and Micro Architecture

Monolithic applications

If all the functionalities of a project exist in a single codebase, then that application is known as a monolithic application. We all must have designed a monolithic application in our lives in which we were given a problem statement and were asked to design a system with various functionalities. We design our application in various layers like presentation, service, and persistence and then deploy that codebase as a single jar/war file. This is nothing but a monolithic application, where “mono” represents the single codebase containing all the required functionalities.

Microservices

It is an architectural development style in which the application is made up of smaller services that handle a small portion of the functionality and data by communicating with each other directly using lightweight protocols like HTTP. According to Sam Newman, “Microservices are the small services that work together.”

The Microservice architecture has a significant impact on the relationship between the application and the database. Instead of sharing a single database with other microservices, each microservice has its own database. It often results in duplication of some data, but having a database per microservice is essential if you want to benefit from this architecture, as it ensures loose coupling. Another advantage of having a separate database per microservice is that each microservice can use the type of database best suited for its needs. Each service offers a secure module boundary so that different services can be written in different programming languages. There are many patterns involved in microservice architecture like service discovery & registry, caching, API gateway & communication, observability, security, etc.

3. Differences between SOAP and REST

SOAP	REST
1.Representational state transfer (REST) is a set of architectural principles used for communication between applications at API level.	1.Simple object access protocol (SOAP) is an official protocol used for communication between applications at API level.
2.It is a protocol with many built-in rules	2.It is not a protocol but rather a set of architectural principles.
3.It is used to build wed services that use different languages.	3.It is also used to build web services that use different languages.
4.It always returns XML files	4.It returns messages in a variety of formats like HTML, XML, plain text, JSON files
5.It is heavy in nature making the applications consume more CPU, RAM.	5.It is lightweight in nature consumes less amount of resources.
6.It has in built security	6.It doesn’t have in built security.